UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/687,320	10/16/2003	Frank J. Hammond II	413130	8493

30955 7590 05/20/2009

LATHROP & GAGE LLP
4845 PEARL EAST CIRCLE
SUITE 201
BOULDER, CO 80301

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
05/20/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/687,320	HAMMOND ET AL.	
	Examiner	Art Unit	
	David Garcia Cervetti	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 February 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 September 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed 2/10/2009 have been fully considered.

2. Claims 1-13 are pending and have been examined.

Response to Amendment

3. Regarding Applicant's arguments, Examiner respectfully points to the teachings of Vallee. Therefore, Vallee teaches the features as follows:

creating a trusted source application to generate and publish encrypted values of a secret and product of first and second large prime numbers (par.96-97, processing done by entity to be authenticated);

reading the encrypted values for the secret and product, by the prover and verifier from the trusted source (par.98, processing done by entity B);

decrypting the secret, by the prover and verifier; decrypting the product, by the prover and verifier (par.100, B verifies response from A); and

performing a plurality of verification dialog between the prover and verifier, wherein the prover demonstrates knowledge of the secret and product without exposing the values of the secret and product, and wherein the client is denied access to a secure area of the host when the prover fails to demonstrate knowledge of the secret and product and granted access to the secure area when the client succeeds in demonstrating knowledge of the secret and product (par.90-108, repeating this a number t times, to authenticate the prover).

4. Regarding the argument that the art does not teach "granting access to an area", the area properly maps to providing or denying services, the services being "secure area", since the services can be information stored for access, thus secure area.

5. Regarding claim 6, Vallee teaches delaying authentication, the values are stored and authenticated later (par.104-108).

6. Regarding the argument against Bartram, Examiner respectfully points out that authentication between peers was conventional and well known, zero-knowledge protocols for authentication were conventional and well known, and someone of ordinary skill in the art would have been able to use one protocol over the other in the system of Bartram with reasonable expectation of success. Bartram provides the architecture to implement authentication between peers, the protocol or algorithm used, is irrelevant. It would have been obvious to someone of ordinary skill in the art to replace Bartram's authentication scheme with other schemes.

7. Regarding the argument that Bartram does not provide an authentication agent and a prover agent, Examiner respectfully submits that these features are at the heart of Bartram's invention, peers, as it is conventional and well known, act as client (prover) and server (authentication), i.e. Bartram teaches that a peer may authenticate other peers, or may authenticate itself to other peers.

8. The cited portion of the specification that support the statement of "admission" are found in the background "zero-knowledge identification protocol" (par.3) and "allows prover to have a set, greater than two, of possible answers, **as is provided by Fiat-Shamir protocol**" (par.10, it admits that Fiat-Shamir exists and was used as

authentication). Thus, the invention is simply implementing Fiat-Shamir on a peer-to-peer environment, as such, Bartram teaches the architecture, and the admission, and state of the art at the time the invention was made, teach to use a zero-knowledge protocol.

9. Assuming arguendo Bartram does not teach what it teaches and the admission is not an admission, Bartram at the very least teaches the architecture, and Vallee teaches using zero-knowledge, therefore, it would have been obvious to someone of ordinary skill in the art to combine the two, to use zero-knowledge protocols on a peer-to-peer environment.

Claim Rejections - 35 USC § 101

10. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

11. Claims 5-7 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

12. Claim(s) 5-7 is/are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The method including steps of ... is broad enough that the claim

could be completely performed mentally, verbally or without a machine nor is any transformation apparent.

Claim Rejections - 35 USC § 102

13. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

14. Claims 5-6 are rejected under 35 U.S.C. 102(e) as being anticipated by Vallee et al. (US 2004/0177252, hereinafter Vallee).

Regarding claim 5, Vallee teaches

a method of protecting a host from unauthorized client access over a network, comprising the steps of (abstract, authentication):

installing a prover agent application on the client (par.7-12, entity to be authenticated);

installing a verifier agent application on the host (par.7-12, authenticator);

creating a trusted source application to generate and publish encrypted values of a secret and product of first and second large prime numbers; reading the encrypted values for the secret and product, by the prover and verifier from the trusted source; decrypting the secret, by the prover and verifier; decrypting the product, by the prover and verifier; and performing a plurality of verification dialog between the prover and

verifier, wherein the prover demonstrates knowledge of the secret and product without exposing the values of the secret and product, and wherein the client is denied access to a secure area of the host when the prover fails to demonstrate knowledge of the secret and product and granted access to the secure area when the client succeeds in demonstrating knowledge of the secret and product (par.90-108, Fiat-Shamir protocol).

Regarding claim 6, Vallee teaches wherein the steps of decrypting the secret and product further utilize previous values of the secret and product as operators in the modulus inverse operations (par.90-108, Fiat-Shamir protocol).

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. Claims 1, 3, 8, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bartram et al. (US 2004/0054885, hereinafter Bartram), and further in view of Admission (specification, pages 1-3, USE of zero knowledge protocols).

Regarding claims 1, 8, and 13, Bartram teaches

a method of non-centralized authentication for a computer network, comprising steps of (abstract, peer-to-peer):

establishing a first computer having a first authentication agent and a first prover agent on the computer network (par.26-29, authentication software);

detecting a first authentication request over the computer network from a second computer having a second prover agent (par.26-29, authenticate another unit);

authenticating the second prover agent through a identification protocol (par.26-29, authenticate another unit); and

promoting the second computer with a second authentication agent to perform authentication for the computer network (par.31-32, second unit authenticates third unit for first unit).

Bartram does not expressly disclose that the authentication/ identification protocol is a zero-knowledge protocol.

However, Applicant admits that the **use** of zero knowledge protocols was conventional and well known at the time the invention was made. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to **use** zero knowledge authentication protocols with the invention of Bartram since it would extend authentication capabilities to other devices and other protocols.

Regarding claim 3, the combination of Bartram and Admission teaches detecting a second authentication request over the computer network from a third computer having a third prover agent (par.26-29); authenticating the third prover agent through a zero-knowledge identification protocol with the second authentication agent (par.31-32); and promoting the third computer with a third authentication agent to perform authentication for the computer network (par.31-32).

17. Claims 2, 4, and 9-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bartram and Admission, and further in view of Vallee.

Regarding claims 2 and 9, the combination of Bartram and Admission does not expressly disclose, however, Vallee teaches periodically generating and distributing a new secret to the first and second authentication agents (par.90-108, Fiat-Shamir protocol). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to publish new secrets as taught by Fiat-Shamir with the invention of Bartram. One of ordinary skill in the art would have been motivated to perform such a modification to renew the secret information.

Regarding claim 4, the combination of Bartram and Admission does not expressly disclose, however, Vallee teaches periodically publishing encrypted numbers for the zero-knowledge identification protocol, including the steps of:

generating first and second large prime numbers; calculating a product of the first and second large prime numbers; generating a secret to have a value relatively prime to the product, greater than zero and less than the product; encrypting the product; encrypting the secret; and publishing encrypted values of the secret and product (par.90-108, Fiat-Shamir protocol). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to publish new secrets as taught by Fiat-Shamir with the invention of Bartram. One of ordinary skill in the art would have been motivated to perform such a modification to renew the secret information.

Regarding claim 10, the combination of Bartram and Admission teaches the requesting computer comprising a cell phone (par.2-3).

Regarding claim 11, the combination of Bartram and Admission teaches the computer network comprising one or more of the Internet, a local area network, a communications link, and a wireless network (par.2-3).

Regarding claim 12, the combination of Bartram and Admission teaches the authentication agents and prover agents being installed on each of the computers through common software (par.25-34).

Allowable Subject Matter

18. Claim 7 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David García Cervetti whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Tuesday and Thursday-Friday.
20. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.
21. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David García Cervetti/
Primary Examiner, Art Unit 2436